USDA

ited States
partment of
riculture

Office of the Chief
Information Officer

1400 Independence
Avenue SW

Washington, DC
20250

JUN 12 2007

TO: Agency Chief Information Officers
Agency Deputy Administrators for Management

FROM: David M. Combs
Chief Information Officer

David M. Combs

SUBJECT: Password Policy

This is an update to the memorandum released on November 9, 2006, which aligned the Department's password policy with NIST guidelines. This memorandum clarifies the previous memorandum, and includes password protection criteria for Blackberry and other wireless personal data assistants (PDA). This policy supersedes any previous password policy. Agencies have 90 days from the date of this memorandum to achieve compliance.

Agencies should align procedures and establish controls to enforce the following minimum password settings for non-privileged users. Non-privileged users are users who do not have administrative rights on a system or application. Agencies may elect to establish more stringent password controls than those specified below.

- Ninety days maximum age limit;
- One day minimum age limit;
- Eight or more characters in length;
- Alpha, numeric, and special character combination (at least one of each);
- No dictionary words;
- Three failed login attempts; and
- A history of five previously used passwords.

Agencies may elect to use a password age of up to 180 days if the following additional criteria is met:

- The password contains a capital letter, lowercase letter, number and special character (at least one of each).

NOTE: Microsoft systems, by default, do not meet the guidelines for 180 day password. These requirements can be met by applying a patch from the National Security Agency (NSA). Please contact the Cyber Security Operations Division for more information.

Agencies should establish policies and controls to enforce the following password settings for privileged user accounts. Privileged users are users who have administrative type access for all or part of an operating system or application.

- Ninety days maximum age limit;
- One day minimum age limit;
- Twelve or more characters in length;
- Alpha, numeric, and special character combination (at least one of each);
- No dictionary words;
- Three failed login attempts; and
- A history of five previously used passwords.

Privileged account holders should have at least two accounts, one account for privileged use and one for common network use such as e-mail and Internet access. Privileged accounts should not be mail or Internet enabled.

Blackberry devices are required to lock after 30 minutes and require a password to be unlocked. The password must meet the following guidelines.

- A minimum of five characters must be used, at least one letter (lower or upper case) and one number must be used (the Blackberry Enterprise Server (BES) must be configured to enforce this policy);
- If six or more characters are used, the password may contain only numbers;
- A minimum of ten failed password attempts before the device is wiped (the Blackberry server must be configured to enforce this policy); and
- Passwords must be changed every 90 days.

Agencies should establish procedures to remotely wipe all lost or stolen Blackberry devices upon notification.

For PDAs that employ Palm OS Version 5 Garnet and Version 6 Cobalt, the device password protection should be set to automatically lock the device on power off and after 15 minutes of inactivity.

Windows Mobile devices including Pocket PCs are required to have a password policy that meets the following requirements:

- Eight or more characters
- Combination of letters and numbers
- Number of incorrect password attempts set to three before the device is wiped
- Lock the device after 15 minutes of inactivity

Two Cyber Security Manual (DM 3500) chapters are affected by this policy change:

- DM 3530-002, Chapter 6, Part 2 IBM and IBM Compatible Security Standards, Section 3, Security Standards, Item G; and

- DM 3535-001, USDA's C2 Level of Trust, Section 3 Procedures, a (1), second paragraph.

Several USDA risk assessment vulnerability checklists are also affected by this policy change. They include:

- USDA Vulnerability Checklist for Telecommunications Systems (August 3, 2001);
- USDA Vulnerability Checklist for UNIX Systems (August 15, 2001);
- Personnel Electronic Device (PED) Security Assessment Guide (September 6, 2001);
- USDA Risk Assessment Checklist for the Novell Network Operating System (NOS) (August 28, 2003); and
- USDA Risk Assessment Checklist for Windows 2000 Domain Controller Server (May 22, 2003).

Agencies should follow this policy memorandum until the above referenced documents can be updated.

Please contact the Computer Security Operations Division at 816-926-7330 for questions or comments regarding this memorandum.